RK

The opinion in support of the decision being entered today was not written for publication and is not binding precedent of the Board.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte BJORN MARKUS JAKOBSSON and CLAUS PETER SCHNORR

Appeal No. 2005-0986
Application No. 09/727,904

ON BRIEF

Before THOMAS, KRASS and DIXON, Administrative Patent Judges.

KRASS, Administrative Patent Judge.

Decision On Appeal

This is a decision on appeal from the final rejection of claims 1-20.

The invention is concerned with electronic information retrieval. In particular, access to information items purchasable from a merchant and accessible over a network is controlled so that even the merchant is unable to identify the

given information item purchased by the user, resulting in complete privacy for the user.

Representative independent claim 1 is reproduced as follows:

1. A method for controlling access to one or more information items purchasable from a merchant and accessible over a network, wherein a user interested in a given information item is permitted to access a corresponding signed ciphertext of the given information item, the signed ciphertext having at least a first ciphertext portion, the method comprising the steps of:

receiving from the user a blinded version of the first ciphertext portion of the signed ciphertext in conjunction with a request from the user for purchase of the given information item from the merchant; and

decrypting the blinded version of the first ciphertext portion and returning to the user the resulting decrypted blinded version of the first ciphertext portion, wherein the resulting decrypted blinded version provides information that is utilized by the user in conjunction with accessing the given information item in a manner such that the merchant is unable to identify the given information item purchased by the user.

The examiner relies on the following references:

Nishioka et al. (Nishioka)	5,754,656	May 19, 1998
Kyojima et al. (Kyojima)	6,275,936	Aug. 14, 2001 (filed Oct. 15, 1998)
Zheng	6,396,928	May 28, 2002 (filed Oct. 24, 1997)

Claims 1-20 stand rejected under 35 U.S.C. § 103. As evidence of obviousness, the examiner offers Nishioka and Kyojima

with regard to claims 1-4, and 7-20, adding Zheng with regard to claims 5 and 6.

Reference is made to the brief and answer for the respective positions of appellants and the examiner.

OPINION

In rejecting claims under 35 U.S.C. § 103, the examiner bears the initial burden of presenting a prima facie case of obviousness. See In re Rijckaert, 9 F.3d 1531, 1532, 28 USPQ2d 1955, 1956 (Fed. Cir. 1993). To reach a conclusion of obviousness under § 103, the examiner must produce a factual basis supported by a teaching in a prior art reference or shown to be common knowledge of unquestionable demonstration. Our reviewing court requires this evidence in order to establish a prima facie case. In re Piasecki, 745 F.2d 1468, 1471-72, 223 USPQ 785, 787-88 (Fed. Cir. 1984). The examiner may satisfy his/her burden only by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead the individual to combine the relevant teachings of the references. In re Fine, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988).

In the instant case, anent independent claim 1, the examiner contends that Nishioka does not explicitly disclose the use of a

blinded ciphertext technique, but does disclose, at column 13, lines 48-52, receiving from the user a first ciphertext portion of the signed ciphertext, and, at column 3, lines 16-61, and, at column 11, lines 15-67, that the user receives this in conjunction with a request from the user for purchase of the given information item from the merchant. The examiner further contends that Nishioka discloses, at column 2, lines 33-67, and column 7, lines 42-62, decrypting the first ciphertext portion and returning to the user the resulting decrypted version of the first ciphertext portion, wherein the resulting decrypted portion provides information that is utilized by the user in conjunction with accessing the given information item in a manner such that the merchant is unable to identify the given information item purchased by the user.

In order to supply the alleged deficiency in Nishioka, the examiner turns to Kyojima for authenticating and controlling access to digital data by applying a blinding effect and decryption technique to ciphertext that can securely transmit a specific piece of information to a decryption device while keeping the blindness of the data to be delegated (pointing to column 4, lines 57-65, column 6, lines 1-7, and 33-45, and column 8, lines 5-41, of Kyojima). The examiner alleges that Kyojima

provides evidence that the artisan would have recognized the benefit of utilizing a blind ciphertext decryption technique to provide for access to digital data while, at the same time, disclosing only the information necessary to perform the intended transaction and protecting "challenging data" such as user identity, specific fees, or purchase price (pointing to column 11, lines 25-65, and column 12, lines 10-18, of Kyojima) (answer-page 4).

The examiner then concludes that it would have been obvious to modify the method of Nishioka to include the blind decryption technique "because it would provide further privacy to a user purchasing an information item since the content of the delegated encrypted key and the decryption key of the digital data cannot be known to the proving device, as per teachings of Kyojima." The examiner points to column 2, lines 2-4, of Kyojima for the motivation of providing for the privacy of a recipient of data, and to column 2, lines 15-25, for a teaching of the seriousness of the privacy problem being exacerbated when decryption of data is occurring over a network.

Appellants' view is that the instant claimed invention would not have been obvious, within the meaning of 35 U.S.C. § 103, because neither of the applied references teaches the advantage

of ensuring that no one other than the user is able to determine what particular information item has been purchased. Appellants argue that whereas the examiner admits that Nishioka fails to teach or suggest the claimed use of a blinded version of a first ciphertext portion of a signed ciphertext, and relies on Kyojima to provide these missing teachings, Kyojima, in fact, fails to provide such teachings.

Specifically, appellants contend that there is no teaching in Kyojima regarding the use of a blinded version of a first ciphertext portion of a signed ciphertext of a given information item purchasable from a merchant. Rather, according to appellants, Kyojima merely discloses a particular blind decryption technique, and they have been unable to find any mention in Kyojima of a signed ciphertext, much less a blinded version of a first ciphertext portion of a signed ciphertext, as claimed (brief-page 5).

Moreover, appellants argue, the examiner has not established a "cogent motivation" (brief-page 5) for modifying the reference teachings to reach the claimed invention because neither of the references relates to processing of a blinded version of a first ciphertext portion of a signed ciphertext of a given information item purchasable from a merchant.

Appellants further allege that Nishioka "teaches away" from the claimed invention because the examiner alleges that the reference discloses that selected information relating to a purchase request by a user is only known to a merchant, while the instant claimed invention relates to purchasing an information item wherein that item is unknown to the merchant.

We have reviewed the evidence before us, including the arguments of appellants and the examiner, and we conclude therefrom that the examiner has not established the requisite prima facie case of obviousness under 35 U.S.C. § 103.

Independent claims 1, 16, and 17 each requires the receipt of a "blinded version of the first ciphertext portion of the signed ciphertext." The examiner admits that Nishioka discloses no such thing, relying on Kyojima for such a teaching. Yet, the portions of Kyojima referenced by the examiner refer to a blind decryption technique, but we find no reference in Kyojima to a blinded version of a "ciphertext portion of the signed ciphertext," and the examiner has not convincingly pointed to anything in the references suggesting such. Nishioka refers to "ciphers" and to a "signature" (e.g., column 13, lines 48-49), but we fail to see how a recitation of a "signature" in Nishioka and a description of a blind decryption technique in Kyojima

would result in the suggestion of a user providing a "blinded version of the first ciphertext portion of the signed ciphertext," in conjunction with a request for the purchase of a given information item, as claimed.

Moreover, we agree with appellants that the examiner has not provided sufficient motivation that would have led the artisan to make the proposed combination. In Nishioka, there are three parties concerned with the transaction, a customer, a merchant and a credit card company. Nishioka seeks to keep information anent specific items purchased from the credit card company, but, unlike the instant claimed invention, information relating to the products purchased by a user "can become known to only a retail store" (Nishioka, column 2, lines 43-44). Thus, why would the artisan modify any teaching in Nishioka to keep the information from the retailer, or merchant, when Nishioka specifically provides for the merchant to have this information? And, if we consider the credit card company of Nishioka to be the "merchant," it may be said that purchased product information is kept from the "merchant," but the technique for doing so is different from the method of the instant claims, wherein a user provides a blinded version of the first ciphertext portion of the signed ciphertext in conjunction with a request from the user for

the purchase of the given information item from the merchant; and the blinded version of the first ciphertext portion is decrypted and returned to the user for the user to use in such a manner as to prevent the merchant from identifying the given information item purchased by the user. Nothing in Kyojima remedies this deficiency in Nishioka.

Accordingly, we will not sustain the rejection of claims 1-17 under 35 U.S.C. § 103.

Regarding claims 18-20, these claims do not recite the receipt of a "blinded version of the first ciphertext portion of the signed ciphertext." The examiner, however, employs the same reasoning to reject these claims as was applied to independent claim 1 (see page 8 of the answer).

Yet, while claims 18-20 do not relate to a blinded version of a first ciphertext portion of a signed ciphertext, they all do recite the requirement that a merchant is unable to identify the given information item purchased by the user, and this is the distinguishing feature of claims 18-20 argued by appellants.

Clearly, as discussed supra, Nishioka specifically permits the merchant to identify such information, and we find nothing in Kyojima suggesting any modification to Nishioka whereby a merchant would be unable to identify this information. Such

information is concealed from the credit card company in Nishioka, and, normally, one might not equate the claimed "merchant" with the credit card company of Nishioka because the claims also require that access to the information items "purchasable from a merchant" is controlled. Clearly, the credit card company in Nishioka is not an entity from which information items may be purchased.

However, in view of appellants' admission, at page 4 of the instant specification, that a payment server, which is associated with a merchant in the preferred embodiment, but may also be a third party entity separate from the merchant, we find that the teaching, by Nishioka, of keeping information on the items purchased secret from the credit card company clearly would have suggested the claimed subject matter whereby a merchant is unable to identify the given information item purchased by the user. Keeping information from one entity would clearly have suggested the ability and desire to keep said information from any other entity. Moreover, a payment server, such as a credit card company, may very well be associated with a merchant, as indicated, for example, by appellants at page 4 of the specification. Where, for example, a credit card company sells items, the "merchant" and the credit card company are one and the

same entity. We note, again, that, unlike independent claims 1, 16, and 17, claims 18-20 do not specify the particular technique employing a blinded version of a first ciphertext portion of a signed ciphertext.

Thus, while we have not sustained the rejection of claims 1-17 under 35 U.S.C. § 103, we will sustain the rejection of claims 18-20 under 35 U.S.C. § 103 because appellants have not convincingly shown any error in the examiner's position.

The examiner's decision is affirmed-in-part.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 CFR § 1.136(a)(1)(iv).

AFFIRMED-IN-PART

JAMES D. THOMAS)
Administrative Patent Judge)
)
)
)
) BOARD OF PATENT
ERROL A. KRASS) APPEALS
Administrative Patent Judge) AND
) INTERFERENCES
)
)
)
JOSEPH L. DIXON)
Administrative Patent Judge)

EK/RWK

JOSEPH B. RYAN
RYAN, MASON & LEWIS, LLP
90 FOREST AVENUE
LOCUST VALLEY, NY 11560